Advisera

Article

ISO 42001 Checklist of Implementation Steps

By Dejan Kosutic

If you're considering how to implement ISO 42001, in the article below you'll find 18 steps that will show you the optimal way to fully comply with this AI governance standard and go for the certification audit.

The best practice to implement ISO 42001 is to follow 18 steps that start with obtaining management support, and end with management review and corrective actions.

1) Obtain management support (clause 5.1)

It sounds obvious, but lack of senior management commitment is the number one reason Artificial Intelligence Management System (AIMS) projects stall. You'll need people, time, and budget — and also management's input about how AI fits into the company strategy.

For that purpose, you'll need to present to the management the benefits of AIMS implementation — you'll have to explain that the AIMS is, in fact, about AI governance, and AI governance is crucial for making the AI systems trustworthy.

2) Treat it as a project

Implementing an AIMS touches many teams (data, product, legal, IT, security) and usually runs for months.

Define the project manager, deliverables, milestones, and the project sponsor just as you would for any other strategic initiative. Make the AIMS plan visible, and track progress weekly.

3) Define your role for the AI system (clause 4.1)

As part of understanding the context of your company, you should define whether your company is an AI provider, AI producer, AI customer, AI partner, or AI subject — this role is important because it helps you with defining your approach to governing your AI systems.

Related Articles

What is ISO 42001? An overview of the AI governance framework
by Dejan Kosutic

ISO 42001 Requirements: Clauses and Structure
by Dejan Kosutic

ISO 42001 vs. ISO 27001: Similarities and differences
By Dejan Kosutic

To learn what each of these roles means, sign up for this free ISO 42001 Foundations Course.

4) Define stakeholders and their requirements (clause 4.2)

There are various groups of people who have an interest in your AI systems — besides customers, these could also be your employees, regulatory agencies, and even society as a whole. What is important is that you collect their expectations related to AI, because this will drive how you manage your AI systems.

Here you can find a more detailed description of this clause, as well as all of the other clauses: ISO 42001 Requirements: Clauses and Structure.

5) Define the scope (clause 4.3)

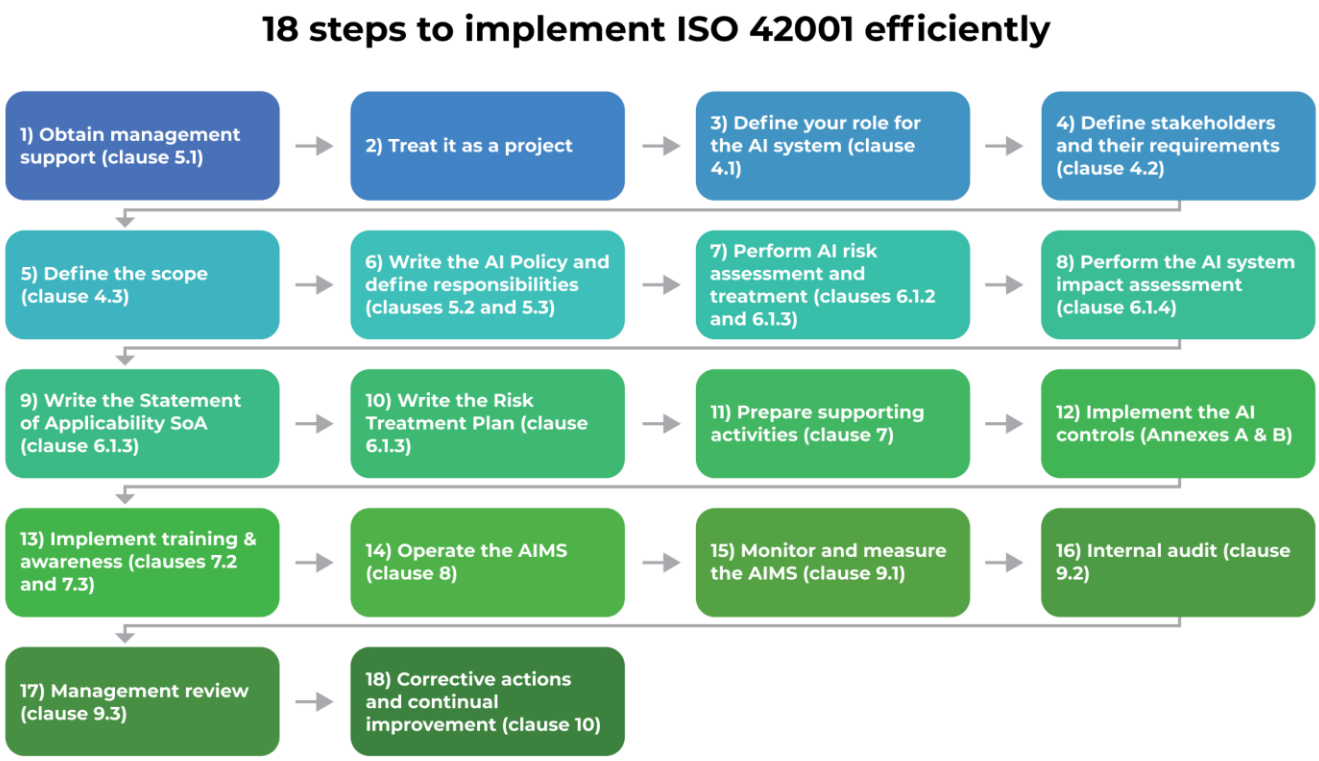
Don't try to do too much at first. Decide which AI systems, products, and departments are in the AIMS scope so that you can focus on those and avoid doing too much.

For example, an e-commerce company could focus only on customer support chatbots, while a bank might focus only on an AI system for credit scoring; alternatively, companies might focus only on AI systems deployed in the EU because of the EU AI Act.

6) Write the AI Policy and define responsibilities (clauses 5.2 and 5.3)

This is your highest-level internal document for AI, and it needs to provide your company's direction for AI governance.

Keep it short, but clear: Specify principles (e.g., fairness, safety), how AI objectives will be defined, main roles and responsibilities, commitments to legal compliance and continual improvement, etc. Make sure you communicate it to everyone.



7) Perform AI risk assessment and treatment (clauses 6.1.2 and 6.1.3)

This is the step that is probably the most complicated. Therefore, before you start doing risk assessment and treatment, you need simple, repeatable rules for identifying, analyzing, and evaluating AI risks: what's "acceptable," how likelihood/impact are assessed, etc. Write those rules in the Risk Management Methodology.

Once you have the methodology, you can start listing all the risks from your AI systems for your company, for individuals, and for society — for each, you have to define the risk level and what kind of AI controls you have to use to decrease those risks. You need to record everything in a Risk Register or some other similar document.

8) Perform the AI system impact assessment (clause 6.1.4)

ISO 42001 requires you to perform an additional, in-depth assessment, called the AI system impact assessment, where you will focus exclusively on what could happen as a consequence of everyday use (or misuse) of your AI systems.

Here you should focus on consequences to individuals and societies, and feed those results into your risk assessment. You should document these results again in the Risk Register, or in a separate document for this particular type of assessment.

9) Write the Statement of Applicability SoA (clause 6.1.3)

In this document, you list all the controls you need and those you're excluding, with justification and how they'll be implemented. Use controls from Annex A as your starting point, and add any additional ones your risks demand.

This document basically summarizes your AI governance activities — in one document, you'll have exactly what you'll do for managing AI and why you're doing this.

10) Write the Risk Treatment Plan (clause 6.1.3)

This is where you turn the SoA into an actionable plan: You need to specify who implements which controls, by when, with what budget, and with which resources.

This is also where you need to get the sign-off from your senior management — not just for this plan, but also for approving the residual AI risks.

11) Prepare supporting activities (clause 7)

For your project to succeed, you'll need to define how the resources are approved and provided — these resources could include money, technology, data, and human resources.

You'll also need to define how the AI governance is communicated throughout the company, but also towards the external stakeholders — who is in charge, and through which means the communication is performed.

Finally, you need to define how you're going to control documents and records — where they will be published, how they're protected, etc.

12) Implement the AI controls (Annexes A & B)

This is the step where you'll spend most of the time and resources, because you need to implement all the controls according to your Risk Treatment Plan.

Typically, these controls are implemented by writing various policies and procedures, but also by purchasing new technologies and performing various other tasks.

As mentioned before, the controls are listed in Annex A; however, in Annex B you have helpful suggestions on how those controls could be implemented.

This free ISO 42001 Foundations Course gives you a detailed breakdown of all the controls.

13) Implement training & awareness (clauses 7.2 and 7.3)

In parallel with your implementation of AI controls, you'll have to explain to your employees why you need all of these controls, as well as how to use them in their everyday work.

This is why awareness (where you give the answer to the question "Why"?) and training (the answer to the question "How?") are crucial — without them, your AI governance will probably fail.

14) Operate the AIMS (clause 8)

Once you implement all the AI controls, you have to start to use (i.e., to operate) them in your daily work — this is when your AI Management System starts to blend with your regular activities.

Even though this is displayed as a step, it is performed continuously — your employees must follow all the AI policies and procedures in their regular work.

15) Monitor and measure the AIMS (clause 9.1)

To know if your AIMS is performing as you expected (for example, if it fulfills the objectives you have set), you have to define how you're going to perform measurement — e.g., specify data sources, frequency, and owners for this activity.

Then you need to start collecting all the data — e.g., track incidents, user satisfaction, system performance, and anything else that you consider important. Then you have to analyze trends and feed results into improvements.

16) Internal audit (clause 9.2)

You must perform the first internal audit before you go for the certification, and then afterwards at least once a year.

Make sure you use an internal auditor who is competent for performing this job, and to create an Internal Audit Report where all the nonconformities are specified.

To learn how to perform internal audits, sign up for this free ISO 42001 Internal Auditor Course.

17) Management review (clause 9.3)

The senior management does not need to handle the details of each AI system, but they must control the overall AIMS — ISO 42001 requires them to do this through a management review.

This management review must use various reports about the AIMS as inputs, and, based on these, the CEO and other senior managers must make crucial decisions about the AI governance — e.g., setting new goals, changes to the budget, new roles and responsibilities, etc.

18) Corrective actions and continual improvement (clause 10)

When something goes wrong, ISO 42001 requires you to find the cause of this nonconformity, and fix this cause, so that the problem does not happen again.

Besides nonconformities, you have to find opportunities to make small improvements to your AIMS — this could be something as simple as correcting your policies and procedures, but also larger things like improving your AI controls, introducing new technologies, etc.

To learn how to implement ISO 42001, sign up for this free ISO 42001 Lead Implementer Course — it will give you a detailed overview of each clause from this AI governance standard, together with practical examples of how to implement them.

About the author:

Dejan Kosutic

Leading expert on cybersecurity & information security and the author of several books, articles, webinars, and courses. As a premier expert, Dejan founded Advisera to help small and medium businesses obtain the resources they need to become compliant with EU regulations and ISO standards. He believes that making complex frameworks easy to understand and simple to use creates a competitive advantage for Advisera's clients, and that AI technology is crucial for achieving this.

Advisera Expert Solutions Ltd
for electronic business and business consulting
www.advisera.com

Our offices

US Office
1178 Broadway, 3rd Floor #3829
New York NY 10001
United States

EU Office
Zavizanska 12
10000 Zagreb
Croatia, European Union

EMAIL:
suport@advisera.com